Asia-Pacific Economic Cooperation

2003/SOMI/ECSG/DPW/013

Addressing Privacy Protection: Charting a Path for APEC

Purpose: Information
Submitted by: Hong Kong, China

APEC Data Privacy Workshop (Panel II)
Chiang Rai, Thailand
13 February 2003

APEC 2003, E-COMMERCE STEERING GROUP

APEC DATA PRIVACY WORKSHOP

on the Subject of

Addressing Privacy Protection: Charting a Path for APEC

~~~~~~~~

A Short Paper on

Implementing Data Privacy Principles:

How Are Governments Making it Work in the Real World?

presented by

Raymond Tang

Privacy Commissioner for Personal Data,

Hong Kong SAR, China

at

Chiang Rai, Thailand

February 13, 2003

****

Introduction

"When there is no privacy, there is no dignity."
~~~~~~~~

The Government of the Hong Kong Special Administrative Region (HKSAR Government) maintains as a policy objective the protection and promotion of the rights of the individual. In pursuing this objective, its target is to achieve local community perception that these rights are safeguarded and on top of that, international community perception that the rights of the individual in Hong Kong are adequately protected.[1]

Privacy as an aspect of fundamental human rights is given general recognition in major international declarations and covenants. Such recognition is also reflected in the constitutional instrument applicable to Hong Kong and in our municipal laws.[2] Whilst the precise scope of privacy which justifies statutory protection remains difficult to define, many jurisdictions, including Hong Kong, have found the prospects of protecting personal data privacy reasonably practicable.

The topic for this Panel is: **"Implementing Data Privacy Principles: How are Governments Making it Work in the Real World?"** I propose to deal with this topic at two levels. At a conceptual level, I shall focus on the implementation of data privacy principles by the (then) Hong Kong Government through the enactment of comprehensive data privacy law in 1995. At a practical level, I shall provide a few life examples of the ways in which my Office (the "PCO") puts the principles into practice in Hong Kong.

Part I : Implementation of data privacy principles through the adoption of comprehensive data privacy law ~ the Hong Kong Experience

(A) Background

The emergence of the concept of protection of personal data is a natural development in the pursuit of economic growth. Hong Kong is

[1] Home Affairs Bureau, Hong Kong : 2001 Policy Address, The Rights of Individuals , available at (http://www.policyaddress.gov.hk/pa01/pdf/righte.pdf).

[2] Article 12, United Nations Universal Declaration of Human Rights; Article 8, European Convention on Human Rights; Article 17, International Covenant on Civil and Political Rights; the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data; Article 14, Hong Kong Bill of Rights Ordinance; Articles 30 & 39, Basic Law of the HKSAR.

internationally recognised as one of the freest economies[3]. The prerequisite of a free economy is the free flow of information. With the development of automatic data processing, the transmission of huge amount of data across national boundaries can be achieved electronically within a matter of seconds or less. The question that follows is how to control or regulate the flow of personal data across national boundaries in an orderly manner that would not put the data privacy rights of the individuals to undue or unacceptable risks.

In an effort to rationalise the international regulation of data flows, the Organisation for Economic Co-operation and Development ("OECD") recommended a set of guidelines on the protection of privacy and transborder flows of personal data ("the OECD Guidelines") on 23 September 1980. Although lacking in legal force in the territorial sense, the OECD Guidelines represent a significant international consensus on the appropriate principles concerning the protection of privacy and individual liberties. The principles adopted in the OECD Guidelines are stated in Appendix I.

Ten years later, on 18 July 1990, the European Commission issued a draft Directive concerning the protection of individuals in relation to the processing of personal data. The aim of the draft Directive is to harmonise the different data protection laws then in force in the European Community and to ensure the free movement of personal data between member states. The draft Directive was finalised and adopted by the European Parliament and of the Council on 24 October 1995[4] ("EU Directive"). The EU Directive requires member states to implement national legislation that meets the Directive's minimum standards of data protection by October 1998[5]. It further prohibits member states from transferring personal data to countries that have no adequate protection of personal data[6]. When assessing a third country's protection, the European Commission will consider all the circumstances surrounding a data

---

[3] The Fraser Institute in its 2002 Annual Report, *Economic Freedom of the World*, ranked 123 entities on 37 variables and placed Hong Kong first.

[4] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of individuals with regard to the Processing of Personal Data and on the Free Movement of such Data, available at (http://europa.eu.int/comm/internal_market/en/dataprot/law/index.htm)

[5] Article 32 of the EU Directives provides: "Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive at the latest at the end of a period of three years from the date of its adoption."

[6] Article 25(1) of the EU Directive provides: "The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection."

transfer, the rules of law in force in the third country in question and the professional rules and security measures actually taken. Up till now, the European Commission has deemed adequate the data protection legislation of Switzerland[7], Hungary[8], and Canada[9] (with Argentina soon to follow suit).

(B) Hong Kong's adoption of statutory control

Faced with the development of data privacy protection in the international arena, Hong Kong moved a step forward on 11 October 1989. On this date, a reference was made to the Law Reform Commission of Hong Kong ("LRC") to consider the subject of "privacy". Its terms of reference were "*to examine existing Hong Kong laws affecting privacy and to report on whether legislative or other measures are required to provide protection against, and to provide remedies in respect of, undue interference with the privacy of individual*....."[10].

The outcome of the LRC's discussion was a recommendation that the internationally agreed data protection guidelines should be given statutory force in ***both*** the public and private sectors[11]. The rationale for this decision was based upon four main arguments.

(a) It was felt that the OECD Guidelines were not comprehensively addressed by any existing legislation in Hong Kong.

(b) The alternative to the statutory regulation of personal data privacy was self-regulation. However, it was felt that this approach would result in inadequate protection to privacy.

---

[7] European Commission Decision 2000/518/EC of 26.7.2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland at (http://europa.eu.int/comm/internal_market/en/dataprot/adequacy/ch_00-518_en.pdf)

[8] European Commission Decision 2000/519/EC of 26.7.2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Hungary at (http://europa.eu.int/comm/internal_market/en/dataprot/adequacy/hu_00-519_en.pdf)

[9] European Commission Decision 2002/2/EC of 20.12.2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act at (http://europa.eu.int/comm/internal_market/en/dataprot/adequacy/canadadecisionen.pdf)

[10] Report on Reform of the Law Relating to the Protection of Personal Data (Topic 27) published by the Law Reform Commission of Hong Kong in August 1994, p.1

[11] Report on Reform of the Law Relating to the Protection of Personal Data (Topic 27) published by the Law Reform Commission of Hong Kong in August 1994, p.66

(c) The international transfer of personal data, that is frequently a prerequisite of international trade, necessitated reciprocal measures if the free flow of data to and from Hong Kong were to be guaranteed.

(d) Hong Kong is a signatory to the International Covenant on Civil and Political Rights ("the ICCPR"). Article 17 of the ICCPR[12] places obligations upon governments to provide statutory protection to defend privacy as a human right. This Article 17 of ICCPR is replicated as Article 14 of the Hong Kong Bills of Right Ordinance (Cap 383 of the Laws of Hong Kong), in so far as it imposes obligations upon the executive government and public authorities.[13] In addition, Article 39 of the Basic Law of the Hong Kong Special Administrative Region[14] places statutory obligations upon the government to implement the provisions of the ICCPR.

The recommendation of the LRC was accepted by the then Administration and Hong Kong opted for a legislative approach to personal data privacy by the enactment of the Personal Data (Privacy) Ordinance (Chapter 486 of the Laws of Hong Kong) ("the PD(P)O") in 1995. The core provisions of the PDPO came into operation on 20 December 1996.

(C) Towards an Internationally Acceptable Standard of Data Privacy Protection

It is now generally accepted that the success of E-commerce depends very much on securing the confidence of consumers over the flow of personal data across territorial boundaries. Such a pre-requisite necessitates the

---

[12] Article 17 of the ICCPR provides that:-

"1. No one shall be subject to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

2. Everyone has the right to the protection of the law against such interference or attacks."

[13] The Hong Kong Bill of Rights Ordinance only binds the Government, all public authorities and any person acting on behalf of the Government or a public authority.

[14] Article 39 of the Basic Law provides as follows:-

"The provisions of the International Covenant on Civil and Political Rights …… shall remain in force and shall be implemented through the laws of the Hong Kong Special Administrative Region.

The rights and freedoms enjoyed by Hong Kong residents shall not be restricted unless as prescribed by law. Such restrictions shall not contravene the provisions of the preceding paragraph of this Article."

The Basic Law of the Hong Kong Special Administrative Region of the Peoples Republic of China was adopted at the third session of the seventh National People's Congress on 4 April 1990 and came into effect on 1 July 1997.

development of standards that will ensure an adequate level of data privacy protection needed to achieve consumer confidence and thus facilitate the introduction and maintenance of E-commerce. In this connection, Hong Kong opted for the adoption of a general law that comprehensively governs the protection of personal data privacy. The adoption of a general law, with territory-wide application, may not be the only option. In other parts of the world, implementation of data privacy principles is done by other means and achieve a level of data protection suited to the territory's needs.

In an ideal world, a common benchmark on data privacy protection (with the necessary mechanism to achieve that benchmark) will enable personal data to be collected, processed and use in manner that would render transborder data flow not an issue. Such state of perfection remains a distant objective. By the nature of things, there are inevitably variations within the community of economies in the areas of culture, economic development, legal and political systems. These variations make difficult the formulation of a common benchmark, much less the acceptance of a common set of standards on implementational mechanism.

Sectoral Laws

Instead of adopting a general law that governs the protection of personal data privacy, some countries prefers to enact specific sectoral laws to protect data privacy. The United States is a good example where sectoral laws are adopted to protect data privacy in certain highly sensitive areas such as financial and medical records, genetic information, social security numbers and information involving children. A distinctive feature of this approach is that new legislation with privacy provisions has to be introduced with the advent of each new initiative.

Self-regulation

By self-regulation, it means that companies and industry bodies establish codes of practice for members to follow. Failure to comply with the codes will be liable for revocation of membership or other forms of disciplinary measures. It was commented that adequacy and enforcement were the major problem with this approach.[15] Consistency with international standard of data

[15] Privacy & Human Rights 2002, EPIC • Privacy International, 2002 edition, p.4

protection presents further challenge when operating under a self-regulatory regime.

The Safe Harbor Agreement

The U.S. Department of Commerce in consultation with the European Commission developed a "safe harbor" framework. Approved by European Commission on 27 July 2000, the "safe harbor" arrangement involves organisations in the U.S. committing themselves to comply with the safe harbor principles backed up by guidance provided through a number of "frequently asked questions". The European Commission recognises that commitment to "safe harbor" will provide an adequate level of protection for transfer of personal data to the U.S. from EU member states.

There are seven safe harbor principles[16], details of which are reproduced at Appendix II. Organisations participating in the safe harbor must comply with the safe harbor's principles and publicly declare that they do so. Each participating organisation has to self-certify annually to the U.S. Department of Commerce in writing that it agrees to adhere to the safe harbor's requirements. It must also state in its privacy policy statement that it adheres to the safe harbor. To enable a party dealing with an organisation to ascertain whether the organisation concerned is participating in the safe harbor framework, a list of the participating organisations and their respective self-certification letters are made available for public inspection by the U.S. Department of Commerce.

How is the safe harbor agreement enforced? Primarily, enforcement will be carried out by the private sector. It is part of the safe harbor obligations that organizations shall have in place a dispute resolution system. Through this system, procedures for verifying compliance will be carried out and complaints and disputes will be resolved upon remedial actions taken. The sanctions that can be imposed by dispute resolution bodies include publicity for findings of non-compliance, suspension from membership and injunctive orders. Failure to comply with the self-regulation requirement is also actionable under federal or state law prohibiting unfair and deceptive acts.

[16] See U.S. Department of Commerce, Safe Harbor at (http://www.export.gov/safeharbor/)

On 13 February 2002, the European Commission published a report[17] on the operation of the "safe harbor" agreement. The report concluded that all the elements of the Safe Harbor arrangement were in place and that individuals were able to lodge complaints if they believed their rights had been denied. However, few had done so and to the Commission's knowledge, no complaint so far remained unresolved. The report further found that a substantial number of organisations that had self-certified adherence to the Safe Harbor were not observing the expected degree of transparency as regards their overall commitment or the contents of their privacy policies. Moreover, there was a wide array of sanctions to enforce Safe Harbor rules under dispute resolution mechanisms but not all of them had indicated publicly their intention to enforce Safe Harbor rules and not all had put in place privacy practices applicable to themselves that were in conformity with the Safe Harbor principles.

In reading the report, however, one should bear in mind that it was published in February 2002. Changes might have been taken place since then. In any event, the Commission will make a full evaluation of the Safe Harbor Agreement in 2003.

Self-Certification Approach

As an alternative, a self-certification[18] approach is proposed to comply with international standard on data privacy protection. Under the proposed scheme, a member country has to accept a declaration by another country framed in the terms of paragraph 17 of the OECD Guidelines - that it substantially observes the Guidelines - as evidence of what it says. Companies incorporated within those countries could then self-certify that they will adhere to the principles. While it is suggested that such a system would have the flexibility to develop privacy law in response to real practical issues, it remains to be seen how is it proposed to prevent declarations being made where there is insufficient, or uncertainty as to sufficiency of, data privacy protection. There is

---

[17] Commission Staff Working Paper: The application of Commission Decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequate protection of personal data provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce, available at (http://europa.eu.int/comm/internal_market/en/dataprot/news/02-196_en.pdf)

[18] Implementing the Data Protection Directive - An Outside Perspective, Peter Ford, First Assistant Secretary, Information and Security Law Division, Attorney-General's Department, Australia, presented at Data Protection Conference and Report on the implementation of Directive 95/46/EC, Brussels, 30 September - 1 October 2002, at p.14-15, at (http://europa.eu.int/comm/internal_market/en/dataprot/lawreport/speeches/ford_en.pdf)

also the added question of how to enforce data privacy in cross border transactions.

(D) A Right Approach for Hong Kong?

In Hong Kong, prior to the enactment of the PD(P)O, the concept of privacy in a modern sense was relatively new to the people of Hong Kong. Without a deeply rooted sense of privacy awareness, the self-regulatory approach which success depends very much on self-initiative, was not regarded as a suitable option for Hong Kong. On top of this lied the obligation on the part of the Hong Kong Government to adopt legislative measures to give effect to the protection of privacy rights. Coupled with the fact that Hong Kong economy could not afford to be competitively disadvantaged by not having a legal data protection regime that met the requirements of the EU Directive, it led to the final adoption of statutory control by the then Hong Kong Government to protect personal data privacy. The advantage of this approach is that control over data privacy protection can be monitored and supervised by a statutory body established to enforce the law. In my view, adopting comprehensive data protection law is an effective way to ensure compliance with data privacy principles by data users. In addition, it provides the legal basis for an individual in seeking redress for data privacy infringement. How effective is this approach? Perhaps its effectiveness is best illustrated by a discussion of the work done by our Office over these years in putting the principles into practice.

Part II : How the PCO puts the principles into practice in Hong Kong?

The purpose of the PD(P)O, as specified in its Long Title, is to protect the privacy of individuals in relation to personal data. Today, except for section 33 (transfer of personal data outside Hong Kong), all provisions under the PD(P)O are in force.

(A) The Legal Framework of PD(P)O

The statutory framework under PD(P)O provides for the establishment of a statutory body to monitor, supervise and promote compliance with the provisions of the PD(P)O, allows the Privacy Commissioner to promote self-regulation through the issuance of Codes of Practice and permits civil redress for any contravention of the provisions of the PD(P)O. The PD(P)O composes of nine parts. The main theme of each part is summarised as follows.

Part I of the PD(P)O give statutory effects to internationally accepted data protection principles. By section 4 of the PD(P)O, a data user is prohibited from doing an act, or engaging in a practice that contravenes a data protection principle unless the act or practice, as the case may be, is required or permitted under the PD(P)O. Schedule 1 to the PD(P)O sets out six data protection principles. They are reproduced at Appendix III.

Part II of the PD(P)O provides for the establishment of a statutory body independent from the government, The Privacy Commissioner for Personal Data.

Part III of the PD(P)O provides for the Privacy Commissioner to approve and issue codes of practice giving guidance on compliance with the PD(P)O.

Part IV of the PD(P)O deals with the power of the Privacy Commissioner to specify classes of data users who are required to provide information concerning their personal data practices for compilation of a public register of data users.

Part V of the PD(P)O confers rights on individuals to obtain access to and to seek correction of their personal data held by data users.

Part VI of the PD(P)O provides controls for automated comparison of personal data, transfer of personal data outside Hong Kong and use of personal data for direct marketing.

Part VII of the PD(P)O confers powers on the Privacy Commissioner to inspect personal data system and to investigate suspected breaches of the PD(P)O. It also provides for the power of the Privacy Commissioner to enter premises, to take evidence, to make reports and to issue enforcement notices.

Part VIII of the PD(P)O contains exemption provisions covering different aspects, including domestic purposes, employment-related data, prevention and detection of crime, assessment and collection of taxes, financial regulation, news reporting, etc.

Part IX of the PD(P)O provides for the legal consequences for breaches of the PD(P)O. Failing to comply with certain provisions may constitute criminal offences. In addition, an individual may institute civil action to claim compensation if he suffers any damage including injury to feelings by reason of a contravention of requirement under the PD(P)O.

(B) The PD(P)O in Practice

Established as an independent statutory body pursuant to the PD(P)O, the PCO is responsible for supervising and enforcing compliance with the law governing data protection privacy in Hong Kong. Its main statutory functions as provided under the PD(P)O are:-

- To monitor and supervise compliance with the provisions of the PD(P)O

- To promote and assist bodies representing data users to prepare codes of practice for guidance in complying with the provisions of the PD(P)O

- To promote awareness and understanding of, and compliance with, the

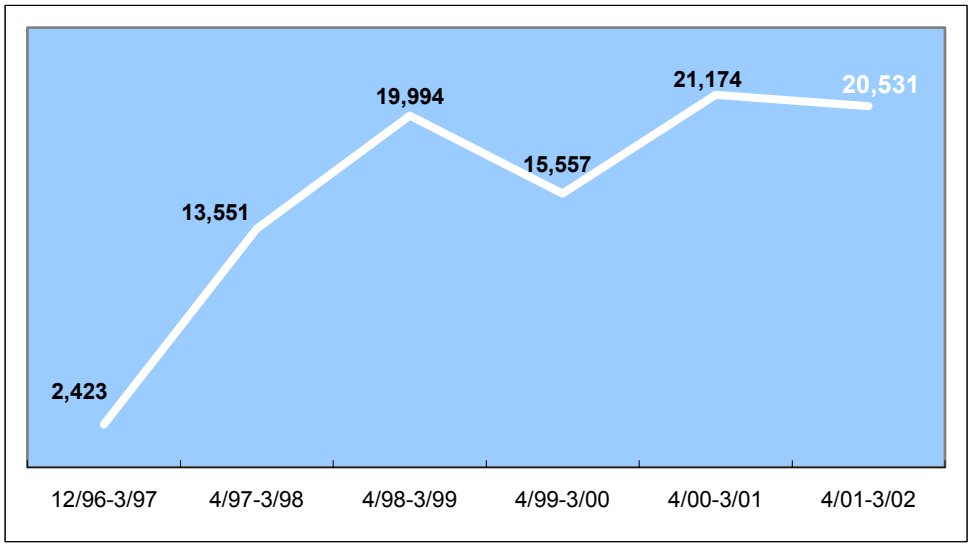
provisions of the PD(P)O

- To liaise and co-operate with counterparts in other jurisdictions

What has been done by the PCO to discharge the above functions to foster data privacy protection in Hong Kong? How the PCO puts the data privacy principles into practice? The answers to these questions may be found in an examination of the work done by the PCO since its establishment in December 1996.

(1) Attending Public Enquiries

Attending to public enquiries is one way to promote awareness and understanding of the requirements of the PD(P)O. Figure 1 shows the number of enquiries we received from December 1996 to March 2002. The total number of enquries attended by PCO in that period amounted to more than 90,000. By the end of 2002, the number had exceeded 100,000 enquiries.

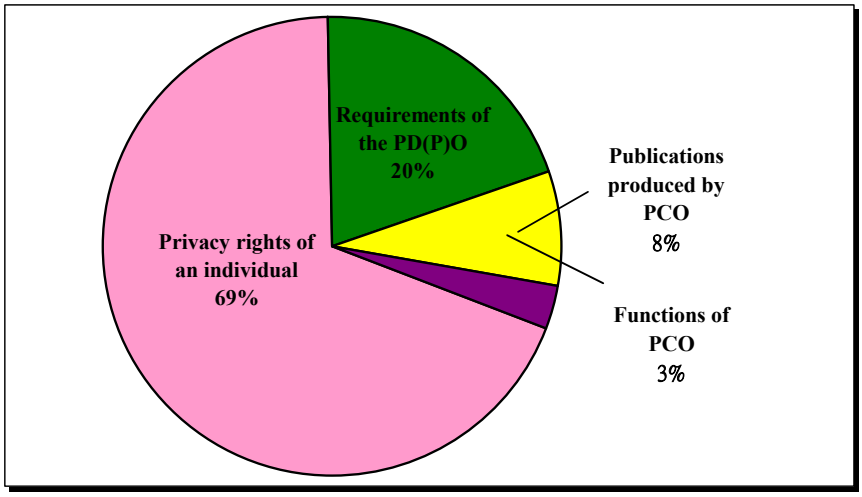


[Fig. 1]

In the year 2001-02, the PCO handled a total of 20,531. On average, some 75 enquiries were received per working day! This is a heavy workload for us given our tight resources.

Figure 2 shows the nature of enquiry cases we received in the year 2001-02.

[Fig. 2]

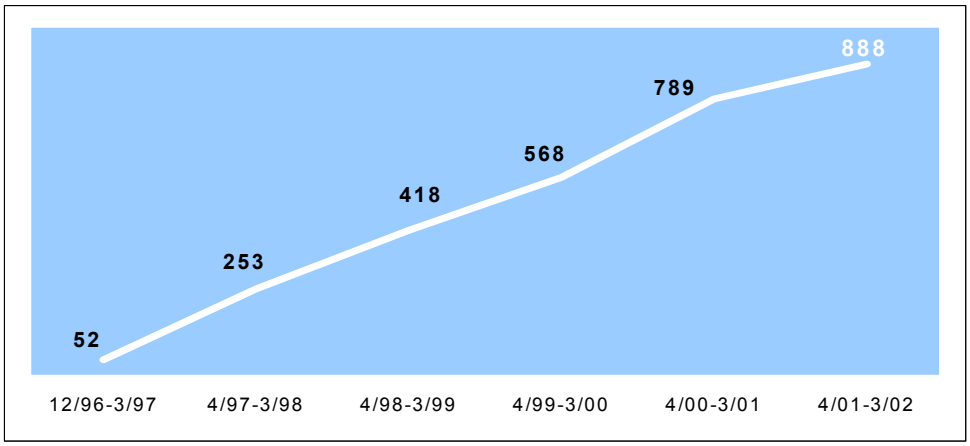


Of the 20,531 enquiry cases, 69% (13,923) related to privacy rights specific to an individual's own situation, 20% (4,204) related to the application of the requirements of the PD(P)O, 8% related to publications we issued and the remaining 3% concerned the function of the PCO.

(2) Handling Complaints

One way to seek redress by an individual for data privacy infringement is to lodge a complaint with the PCO. The PD(P)O confers specific powers on the Privacy Commissioner to carry out investigation of complaints and to take appropriate enforcement actions upon completion of investigation of complaints.

Figure 3 shows the number of complaints we received from December 1996 to March 2002.

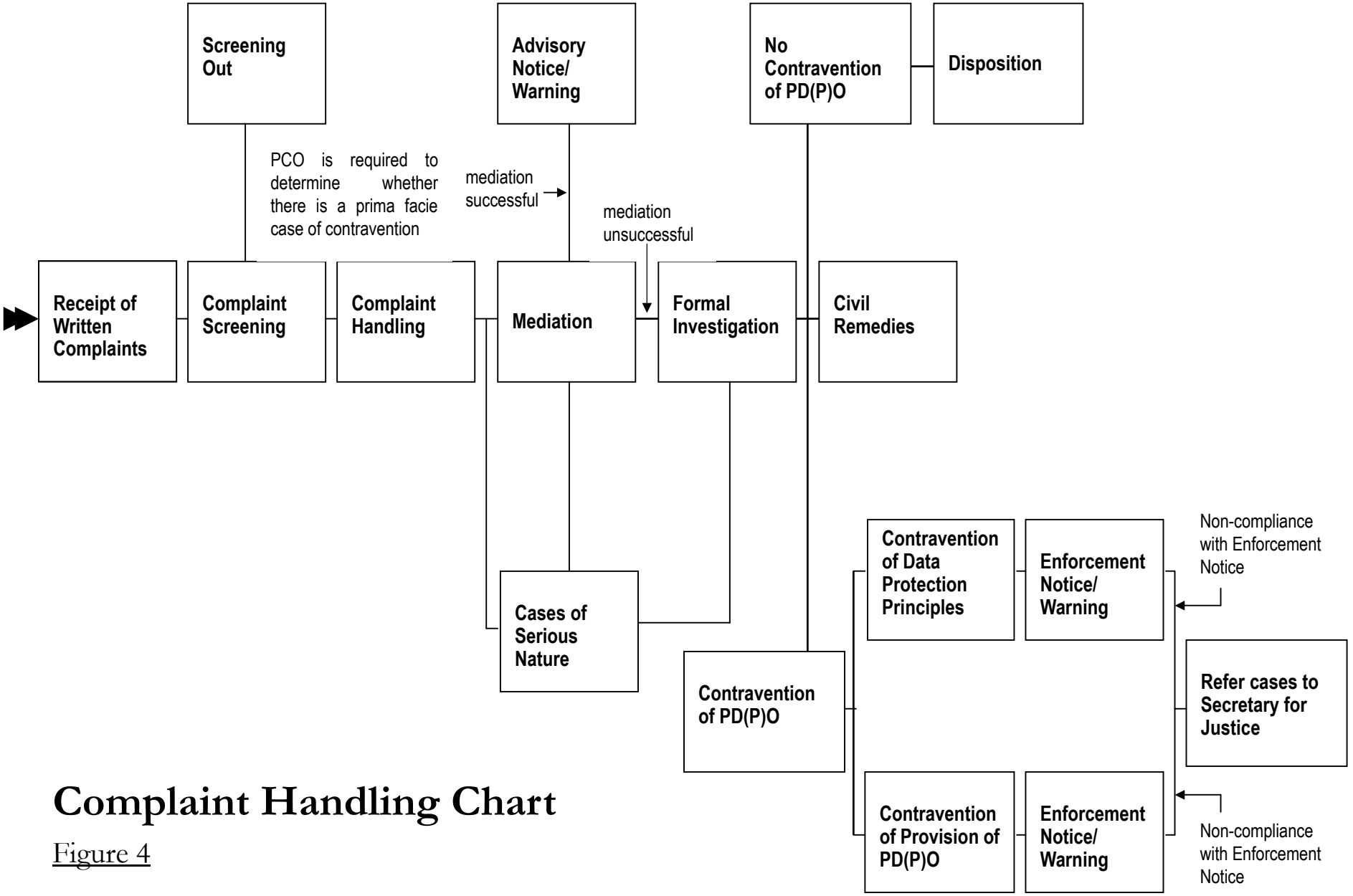


[Fig. 3]

Since the PD(P)O came into effect on 20 December 1996, the PCO has handled more than 3,700 complaints lodged by individuals who suspected that their privacy rights have been infringed. In the year 2001-02, we received 888 formal complaints of possible breaches of the PD(P)O. Compared with 789 complaints received in 2000-01. This represents a 12% yearly increase in the complaint caseload.

What can the PCO do to assist a complainant? What are the enforcement actions taken by the PCO? A good start on the discussion of these questions is to understand the workflow of the PCO on complaint handling.

Figure 4 shows the Complaint Handling Procedures of PCO.



Complaint Handling Chart

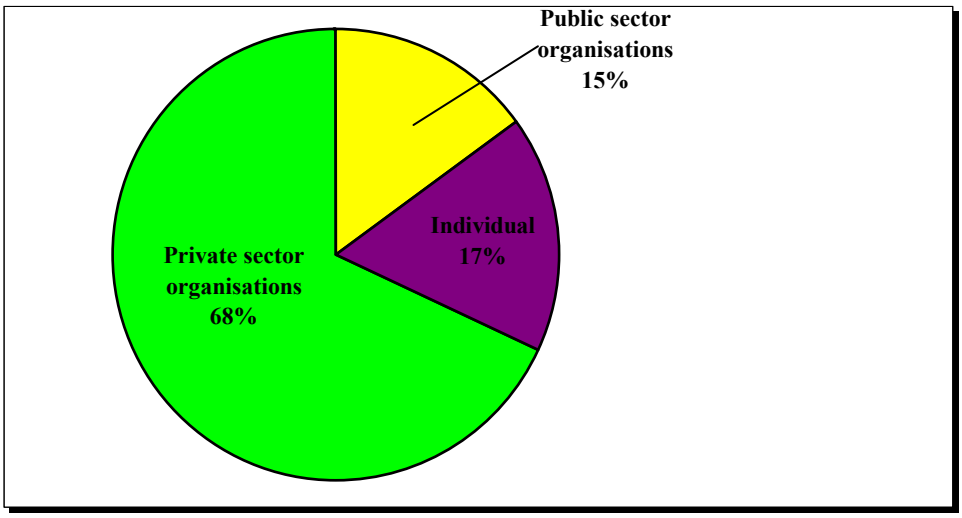
Figure 4

(a) Complaint Handling Procedures

Having received a complaint, the PCO will first carry out a preliminary inquiry with the parties involved in the complaint including not only the complainant and the party complained against but also any witnesses who may be able to provide information relevant to the complaint. This procedure is to obtain evidence from the relevant parties so that the investigation officer may determine from the evidence whether a *prima facie* case of contravention of the requirement of PD(P)O is established.

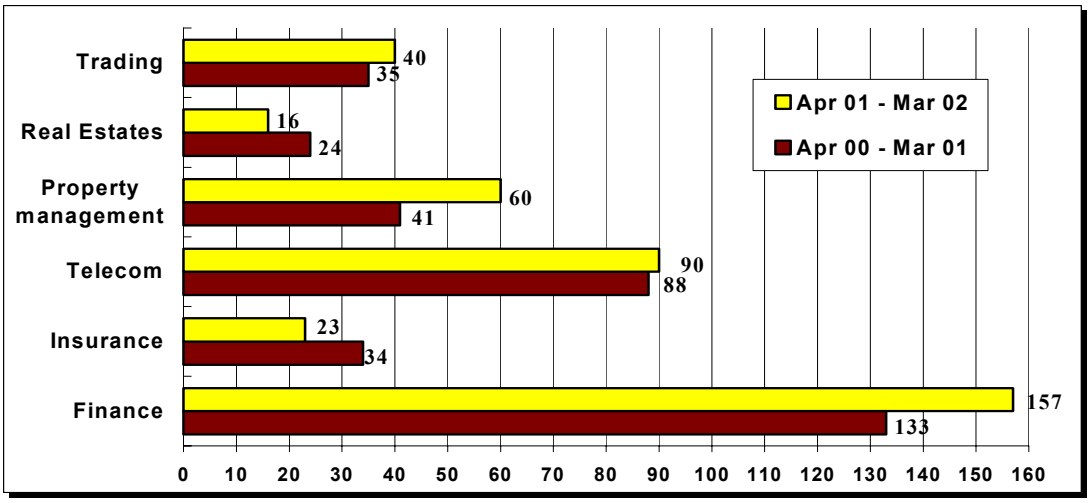
If there is no *prima facie* case established, the complainant will be notified that no further action will be taken by the PCO in relation to his complaint. On the other hand, if there is *prima facie* case established and the nature of complaint is not serious, the PCO will try to resolve the dispute through mediation. If the dispute cannot be resolved through mediation or if the nature of the complaint is serious, a formal investigation will be carried out, to be followed by enforcement action where necessary.

Figure 5 shows the classification of party complained against in the year April 2001- March 2002.

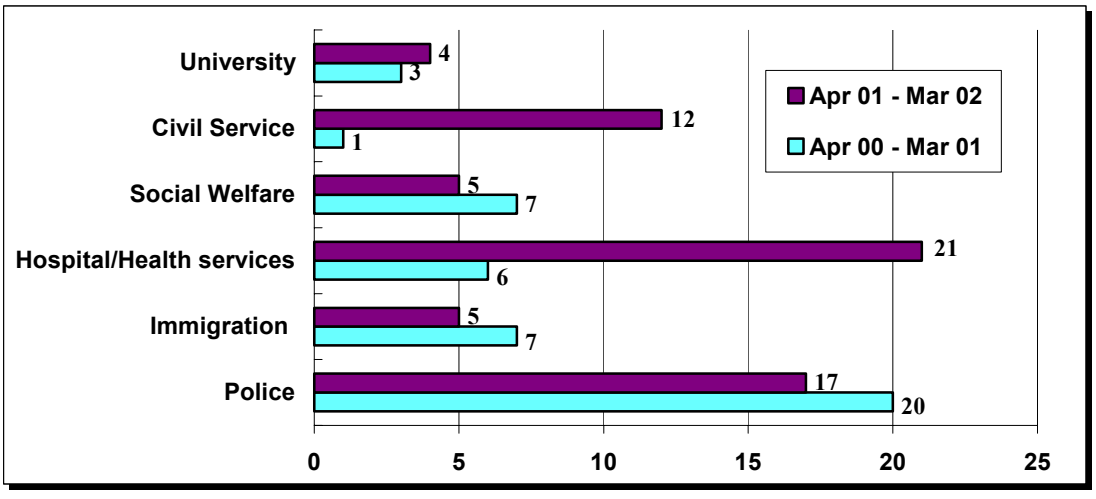


[Fig. 5]

Of the 888 complaints we received in 2001-02, 68% were complaints against private sector organizations, 15% were complaints against public sector organizations, the remaining 17% were complaints lodged against third party individuals. Figure 6 shows the breakdown of complaints against the most significant private sector organisations and Figure 7 shows the breakdown of complaints against the most significant public sector organisations.

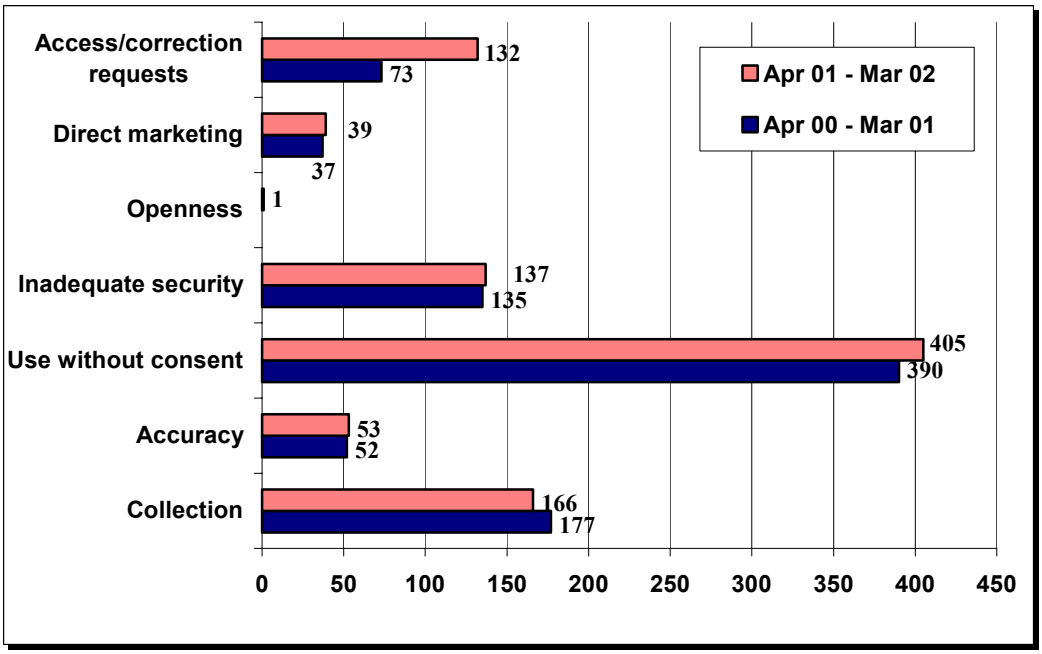


[Fig. 6]



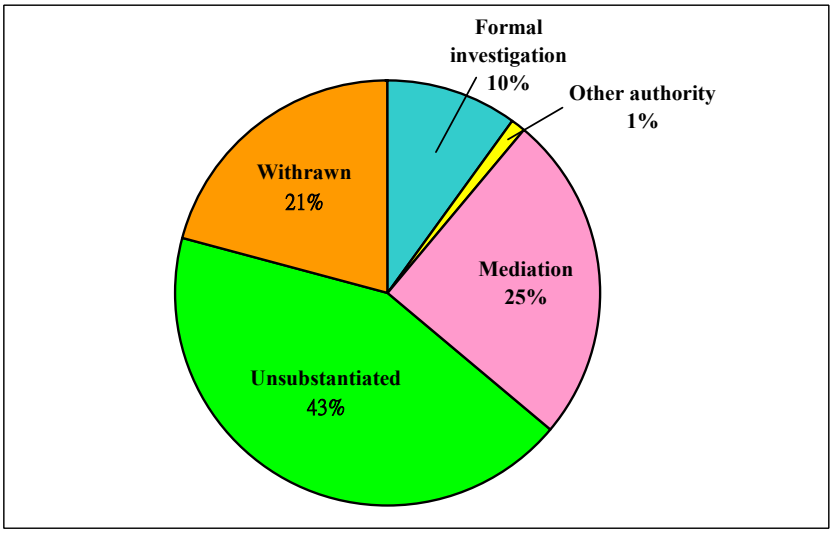
[Fig. 7]

As regards the nature of complaints received in the 2000-01 and 2001-02, please see Figure 8 below:



[Fig. 8]

The highest number of complaints is made against alleged use of personal data without consent. The next highest is allegations of unfair and excessive collection of personal data, then followed by inadequate security protection of personal data. Figure 9 shows the outcome of complaints investigated by PCO in the year April 2001 to March 2002.



[Fig. 9]

There were a total of 483 complaint cases completed by PCO in the year 2001-02. Of these, 123 cases (25%) were resolved through mediation, 48 cases (10%) were resolved after formal investigations, 204 cases (43%) were found to be unsubstantiated as a result of investigation and 102 cases (21%) were withdrawn by the complainants during investigation. The remaining 6 cases (1%) involved complaints which the complainants had also referred to other authorities to follow up.

(b) Mediated Settlement

One can see that a majority of complaints handled by PCO in 2001-02 were resolved through mediation. In this process, following a preliminary inquiry of a complaint, the PCO will form a preliminary view on the matter complained of based on the evidence available. The PCO will notify the party complained against of such view and request it to undertake remedial actions to remedy the matter complained of. If the party complained against agrees to take the remedial actions, the complaint will be considered as resolved through mediation. For illustration purpose, I state below a complaint case handled by PCO which was resolved effectively through mediation.

Case 1 – Fee for compliance with a data access request

A patient requested a clinic to provide him with duplicates of 65 clinical slides. The clinic required him to pay almost HK$15,000 (HK$230 per slide). The patient considered the fee excessive and lodged a complaint with PCO.

Section 28 of the PD(P)O permits a data user to impose a fee for complying with a data access request. However, such fee imposed should not be excessive. In our view, in fixing the fee, it would be acceptable to include a reasonable administrative cost in locating the data and the actual expenses incurred in providing copies of the data.

After considering the views of the PCO on how fees for providing copies of personal data should be calculated under section 28 of the PD(P)O, the clinic reviewed its policy, and subsequently reduced the fee to HK$468 (HK$7.20 per slide), representing the actual expenses of producing the slides plus a 20% administrative charge.

(c) Investigation and Enforcement Actions

Where a dispute cannot be resolved through mediation or where the nature of the complaint is serious, the PCO may proceed to undertake a formal investigation. If an investigation confirms that the data user has contravened a requirement under the PD(P)O, an enforcement notice may be served on the relevant data user directing it to take necessary steps to remedy the contravention. It is however worth nothing that the PD(P)O does not confer any power on the Privacy Commissioner to award compensation to the complainant.

Below is a complaint case handled by the PCO where enforcement action was taken.

Case 2 - Sending abusive messages on the Internet

The complainant complained that his ex-colleague, without his knowledge or consent, posted his name and mobile phone number in a message at an Internet newsgroup soliciting sexual service thus resulting in numerous nuisance calls to him. Upon investigation by the PCO, it was ascertained that his ex-colleague obtained his mobile phone number while they were employees of the same company. Although the sender of the message tried to hide his identity by using a fake account name, the PCO secured evidence from the related Internet Service Provider that the account from which the message originated was that of the ex-colleague. An enforcement notice was served on the ex-colleagues directing him to cease such action.

(d) Consequence of failing to comply with an enforcement notice

Pursuant to section 64(7) of the PD(P)O, any relevant data user who contravenes an enforcement notice served on the data user commits an offence and is liable on conviction to a fine[19] and to imprisonment[20]. In case where a data user who has been served with an enforcement notice fails to comply with the terms of the enforcement notice, the PCO will refer the case to the Hong Kong Police for investigation and prosecution. Below is a case where a data user was convicted and fined for failure to comply with an enforcement notice.

Case 3 - Unfair collection of customers' data

---

[19] By virtue of section 113B and Schedule 8 of the Criminal Procedure Ordinance (Chapter 221 of the Laws of Hong Kong), the current maximum penalty applicable is HK$50,000.

[20] Pursuant to section 64(7) of the PD(P)O, the maximum imprisonment sentence is 2 years.

The complainant complained that a former hotel telesales consultant had unfairly collected his personal data. The complainant first received a direct marketing call from the telesales consultant who promoted membership packages of the hotel. After being offered very attractive membership packages, the complainant agreed to join the membership and gave her personal particulars to the telesales consultant. However, she later discovered that the terms of the scheme were totally different to what was promised by the telesales consultant and therefore lodged a complaint to the hotel. The telesales consultant was subsequently dismissed by the hotel. Feeling aggrieved, he took into his possession records of the complainant's personal data and used the data to send out numerous fax letters to the complainant accusing her of causing him to lose the job.

After investigation, the telesales consultant was found to have contravened Data Protection Principle 1(2) of the PD(P)O by having collected the complainant's personal data by unlawful or unfair means. An enforcement notice was served on him directing him to retrieve this customer's information to the hotel. He however failed to comply with the enforcement notice. The case was then referred to the police for their consideration of prosecution proceedings pursuant to the section 64(7) of the PD(P)O.

The telesales consultant denied having received the enforcement notice but during an identification parade he was positively identified by our officer who served the enforcement notice on him at the material time. The telesales consultant was accordingly charged. At the hearing, he was convicted and fined for failure to comply with the enforcement notice.

(e) Publication of a report

Pursuant to section 48(2) of the PD(P)O, after completing an investigation, if the Privacy Commissioner is of the opinion that it is in the public interest to do so, a report may be published setting out the results of the investigation and the recommendations or comments arising from the investigation. As a sanction to the relevant data user, the identity of the relevant data user may be disclosed in the report.

Below is a case where a report was published by the PCO after completion of an investigation of a complaint.

Case 4 – Covert video-taping of person in a private place

A student at a university discovered that she had been covertly videotaped in her hostel room. A video camera, covered by a box, was placed on top of a cabinet in the room which she shared with a fellow-student. The camera was loaded with a videotape that had already captured some images of hers. She complained to the PCO.

Data Protection Principle 1(2)(b) requires that personal data should be collected by means that are fair in the circumstances of the case. In the absence of any overriding public interest, it is unfair to photograph or video-tape a person's image in a private place with an intent to collect that person's personal data without that person's knowledge or consent. In addition, the disclosure of the complainant's video image to other persons in the absence of her consent contravened Data Protection Principle 3.

Investigation revealed that the video camera had been placed there by a friend of the fellow-student. He admitted that he had collected images of the complainant by such means on three occasions over a period of several months. He claimed that his purpose in videotaping the complainant's activities in the room was to collect evidence of the presence of someone known to the complainant on the said premises without proper authority. He further admitted that he had shown one of the tapes to a friend.

An enforcement notice was served on the person complained against directing him to retrieve and surrender to the complainant any video-tapes made of the complainant and cease duplicating, using or showing any such tapes to any other person.

(3) Compliance Check

To discharge its function to monitor and supervise compliance with the requirements of the PD(P)O, the PCO finds that it is not adequate only to take a passive role in waiting for complaints lodged by individuals. From time to time, the PCO will take its own initiative to carry out compliance check to oversee the compliance with the requirements of the PD(P)O by data users. A compliance check is undertaken when the PCO identifies a practice in an organisation that appears to be inconsistent with the requirements of the PD(P)O. In such circumstances, the PCO raises the matter in writing with the organization concerned pointing out the apparent inconsistency and inviting it, where appropriate, to take remedial action. In many cases, the organisations concerned will take the initiative and respond by undertaking immediate actions to remedy

the suspected breaches. In other cases, organisations seek advice from the PCO on the improvement measures that should be adopted to avoid a repetition of the suspected breaches.

We have done more than 300 compliance checks since our establishment. Organisations that have been subjected to our compliance checks include government departments, public utilities, financial institutions, telecommunications companies, property management companies and insurance companies. In 2001-02, the PCO conducted 41 compliance checks in relation to the alleged practices of data users that might be inconsistent with the requirements of the PD(P)O. Of these, 5 compliance checks related to practices in government departments or statutory bodies. The remaining 36 compliance checks related to practices in private sector organisations. For further understanding of the compliance checks undertaken by the PCO, please see the list attached at Appendix IV.

(4) Codes of Practice

The PCO recognises the importance of giving practical guidance to data users on how to comply with data protection principles which are worded in generic terms. In this connection, section 12(1) of the PD(P)O provides that the Privacy Commissioner may, for the purpose of providing guidance in respect of any requirements under the PD(P)O, approve and issue codes of practice. The preparation of such a code may be done by a particular sector or profession or by the Privacy Commissioner. Before approving a code of practice, the Privacy Commissioner is required to consult such representative bodies of data users to which the code will apply and such other interested persons as he thinks fit.

A contravention of a code of practice approved by the Privacy Commissioner does not of itself constitute a breach of the PD(P)O. However, it will give rise to a presumption against the data user in any legal proceedings under the PD(P)O.

As at today, the codes of practice approved by the Privacy Commissioner consist of the following:-

(a) Code of Practice on the Identity Card Number and other Personal Identifiers

By virtue of section 12(8) of the PD(P)O, the Privacy Commissioner is required to approve a code of practice giving practical guidance on the application of the PD(P)O to personal data that are personal identifiers, including the identity card number. A code of practice was thus approved and issued on this subject. The code contains provisions dealing with the collection, retention, accuracy, use and security of the identity card number, copies of identity card and other personal identifiers.

(b) Code of Practice on Consumer Credit Data

This code relates to personal data shared between financial institutions and credit reference agencies. The issuance of this code was prompted by a recognition of the sensitivity of information related to the creditworthiness of an individual and the potentially far-reaching consequences for that individual if credit is refused on the basis of such information. Before the issuance of the code, the operations of credit reference agencies were not subject to direct regulatory control. The code deals with the handling by credit providers, credit reference agencies and debt collection agencies of personal data related to consumer credit transactions.

(c) Code of Practice on Human Resources Management

This code aims at providing practical guidance on compliance with the data protection principles in all aspects of human resource management activities, dealing with recruitment, current employees' matters and former employees matters. In particular, the code prohibits the use of "blind" recruitment advertisements, i.e. advertisements that do not reveal the identity of the advertisers and yet directly solicit the submission of personal data from applicants. It also proposes different retention periods for various types of employment-related personal data.

Another code of practice which the PCO is actively working on is the Code of Practice on Monitoring and Personal Data Privacy at Work. This code aims at giving practical guidance on the application of the requirements of the

PD(P)O to employee monitoring involving personal data. A consultation on the draft code was concluded last year.

(5) Matching Procedures

A matching procedure is the automated matching of personal data of ten or more individuals collected for different purposes with a view to taking adverse action against one or more of them. Adverse action means, in turn, any action that may adversely affect an individual's rights, benefits, privileges, obligations or interest, including legitimate expectations.

Section 30 of the PD(P)O prohibits the carrying out of matching procedures by data users unless any one of the following conditions has been met:-

(a) all the individuals who are the subjects of the data to be matched have voluntarily given express consent to the matching procedure being carried out;

(b) the Privacy Commissioner has given consent for the matching procedure to be carried out;

(c) the matching procedure belongs to a class of matching procedures which the Privacy Commissioner has specified by notice in the Government Gazette as a class of such procedures that may be carried out; or

(d) the matching procedure is required or permitted by a provision of another Ordinance specified in schedule 4 to the PD(P)O.

Up till now, no matching procedures under condition (c) or (d) has been specified. Accordingly, in order for a data user to carry out a matching procedure in compliance with section 30, either the data subject's consent has to be sought or the Privacy Commissioner's approval has to be obtained. It ensures that no data user can carry out a matching procedure in the dark. Any person who without reasonable excuse carries out a matching procedure in contravention to section 30 of the PD(P)O commits an offence.

To approve the carrying out of a matching procedure is in essence to allow the change of use of personal data without the data subjects' consent. In considering whether to approve an application, the Privacy Commissioner has

been extremely careful in exercising his discretion conferred under the PD(P)O. The following are the matters that will be taken into account by the Privacy Commissioner:-

(i) whether the carrying out of the matching procedure is in the public interest;

(ii) the kind of personal data to be the subject of the matching procedure;

(iii) the likely consequences to a data subject if the matching procedure were to result in any adverse action taken against the data subject;

(iv) the practices and procedures, if any, that will be followed to enable a data subject to make a data correction request—
   (a) in respect any of the personal data produced or verified by the matching procedure;
   (b) before any adverse action is taken against the data subject;

(v) the practices and procedures, if any, that will be followed to ensure, so far as is practicable, the accuracy of any personal data produced or verified by the matching procedure;

(vi) whether any such data subject is to be informed of the procedure before it is first carried out;

(vii) whether there is any practicable alternative to the matching procedure;

(viii) the benefits to be derived from carrying out the matching procedure.

So far, most of the matching procedures approved are all justifiable on the grounds of public interest, for examples, for detection of double housing benefits, for detection of overpayment of social security payments, to identify registered electors who might become ineligible to vote, etc. For details of some of the applications approved by us, please see Appendix V.

(C) Problems encountered by the PCO in the implementation of the PD(P)O

Like other jurisdictions, Hong Kong encountered difficulties in the course of its implementation of the PD(P)O. In the initial stage, the community was generally indifferent to personal data privacy. This was a novel concept to most people in Hong Kong. Secondly, privacy was not high on the government's agenda, as there were more pressing policy portfolios such as housing, social welfare, education and healthcare ahead. Thirdly, there were some misconceptions amongst the business sector that compliance with the PD(P)O would lower the efficiency and hence reduce the competitiveness of the business. To meet this challenge, the solution by PCO was to enhance the awareness of personal data privacy, thus building a culture in Hong Kong which personal data privacy was understood and valued.

Today, having tasted the fruits of personal data privacy protection, the community calls for more protection. It is particularly so amongst the celebrities and artistes who constantly find themselves confronted with the media engaging in paparazzi. The protection offered by the PD(P)O is in relation to "personal data"[21] as specifically defined under the PD(P)O. What the PD(P)O protects is "information privacy", rather than "personal privacy" in a general sense. Bound by the limits under the PD(P)O, the PCO sometimes finds its hands tied in respect of complaints on *personal* privacy infringement. Further thoughts must be directed at the role of the PCO in this area, but perhaps not before the undertaking of a comprehensive review on the scope of protection under the PD(P)O. Nonetheless, the PCO will continue to exercise its best endeavour to handle those complaints within the boundaries of the PD(P)O.

Challenges Ahead ~~ *In Quest of a Common Approach*

While Hong Kong has at times been referred to as a model[22] that combines the best of prescriptive rules and self regulation, there is no hard and fast rule for a government to decide which approach to take in implementing data privacy principles within its own jurisdiction. Whilst due consideration has to be

---

[21] The term "personal data" is defined in section 2(1) of the PD(P)O as "any data (a) relating directly or indirectly to a living individual; (b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and (c) in a form in which access to or processing of the data is practicable".

[22] Re-thinking Information Privacy - A Third Way in Data Protection? Mr Nigel Waters, Privacy Consultant, Pacific Privacy Partners, Australia, presented at 21st International Conference on Privacy and Personal Data Protection, Sept 1999.

given on how to comply with internationally acceptable data protection standards, diverse factors and values within an economy will ultimately shape the model best suited to its community. As evident from the work done by PCO, the approach taken by Hong Kong is consistent with the local community's expectation and it has achieved general acceptance. In the 2001 Opinion Survey[23] done by the Social Sciences Research Centre of the University of Hong Kong, 95% of the respondents either agreed, or strongly agreed with the view that the PCO had been successful in increasing community awareness of personal data privacy issues.

In the context of E-commerce development, transborder data flow becomes an issue which every economy has to deal with sooner rather than later. By definition transborder traffic will impact upon the regulatory regimes of the exporting and importing economies. There lies the need to find a common approach towards data privacy that would not operate as an impediment to the development of cross-border trade. Fulfillment of that need hinges on harmonization.

In Hong Kong, our data protection law incorporated the principal requirements of both the OECD Guidelines (with regard to OECD principles) and the EU Directive (with regard to both principles and mechanism). Our legislation was enacted following the recommendations of the Law Reform Commission after due consideration of local conditions and situations overseas in the early Nineties. At that time, regional and international compatibility in privacy development did not have the same significance as nowadays. With the development of E-commerce the sentiment has changed. The perceived value and benefits of electronic commerce has become the driving force behind the quest to seek compatibility but at the same time highlighted regional diversities towards data privacy. Recognizing the differences in cultural, legal and economical backgrounds within the region, there may now be a case for the development and adoption of a regional standard or common approach towards data protection.

International co-operation is crucial to reducing privacy risks in cross-border data flow. On 27 November 2002, the PCO signed a Memorandum of Understanding (MOU) with the Korea Information Security Agency (KISA)

[23] 2001 Opinion Survey "Personal Data (Privacy) Ordinance: Attitudes and Implementation - Key Findings, available at (http://www.pco.org.hk/english/publications/opinionsurvey.html)

to foster better understanding and co-operation on research on protection of personal data privacy in our respective jurisdictions. It is one of the major objectives of PCO to strengthen its ties with overseas data protection authorities. The signing of the MOU represents a step forward to the creation of a strengthened regional forum for the advancement of personal data protection. Hong Kong will continue to move along this path in advocating personal data privacy.

Office of the Privacy Commissioner for Personal Data
13 February 2003

Appendix I: OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data[24]

PART ONE: GENERAL DEFINITIONS

1. For the purposes of these Guidelines:
   a) "data controller" means a party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf;
   b) "personal data" means any information relating to an identified or identifiable individual (data subject);
   c) "transborder flows of personal data" means movements of personal data across national borders.

Scope of Guidelines

2. These Guidelines apply to personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties.

3. These Guidelines should not be interpreted as preventing:
   a) the application, to different categories of personal data, of different protective measures depending upon their nature and the context in which they are collected, stored, processed or disseminated;
   b) the exclusion from the application of the Guidelines of personal data which obviously do not contain any risk to privacy and individual liberties; or
   c) the application of the Guidelines only to automatic processing of personal data.

4. Exceptions to the Principles contained in Parts Two and Three of these Guidelines, including those relating to national sovereignty, national security and public policy ("ordre public"), should be:
   a) as few as possible, and
   b) made known to the public.

[24] See website of Organisation for Economic Co-operation and Development, available at (http://www.oecd.org/EN/document/0,,EN-document-13-nodirectorate-no-24-10255-13,00.html)

5. In the particular case of Federal countries the observance of these Guidelines may be affected by the division of powers in the Federation.

6. These Guidelines should be regarded as minimum standards which are capable of being supplemented by additional measures for the protection of privacy and individual liberties.

PART TWO: BASIC PRINCIPLES OF NATIONAL APPLICATION

Collection Limitation Principle

7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle

8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle

9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle

10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

a) with the consent of the data subject; or
b) by the authority of law.

Security Safeguards Principle

11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

Openness Principle

12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle

13. An individual should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
b) to have communicated to him, data relating to him
    i. within a reasonable time;
    ii. at a charge, if any, that is not excessive;
    iii. in a reasonable manner; and
    iv. in a form that is readily intelligible to him;
c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and
d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

Accountability Principle

14. A data controller should be accountable for complying with measures which give effect to the principles stated above.

PART THREE: BASIC PRINCIPLES OF INTERNATIONAL APPLICATION: FREE FLOW AND LEGITIMATE RESTRICTIONS

15. Member countries should take into consideration the implications for other Member countries of domestic processing and re-export of personal data.

16. Member countries should take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a Member country, are uninterrupted and secure.

17. A Member country should refrain from restricting transborder flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A Member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other Member country provides no equivalent protection.

18. Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection.

PART FOUR: NATIONAL IMPLEMENTATION

19. In implementing domestically the principles set forth in Parts Two and Three, Member countries should establish legal, administrative or other procedures or institutions for the protection of privacy and individual liberties in respect of personal data. Member countries should in particular endeavour to:

a) adopt appropriate domestic legislation;
b) encourage and support self-regulation, whether in the form of codes of conduct or otherwise;
c) provide for reasonable means for individuals to exercise their rights;
d) provide for adequate sanctions and remedies in case of failures to comply with measures which implement the principles set forth in Parts Two and Three; and
e) ensure that there is no unfair discrimination against data subjects.

PART FIVE: INTERNATIONAL CO-OPERATION

20. Member countries should, where requested, make known to other Member countries details of the observance of the principles set forth in these Guidelines. Member countries should also ensure that procedures for transborder flows of personal data and for the protection of privacy and individual liberties are simple and compatible

with those of other Member countries which comply with these Guidelines.

21. Member countries should establish procedures to facilitate:
    a) information exchange related to these Guidelines, and
    b) mutual assistance in the procedural and investigative matters involved.

22. Member countries should work towards the development of principles, domestic and international, to govern the applicable law in the case of transborder flows of personal data.

Appendix II: Seven Safe Harbor Principles[25]

1. **Notice:** Organisations must notify individuals about the purposes for which they collect and use information about them. They must provide information about how individuals can contact the organisation with any inquiries or complaints, the types of third parties to which it discloses the information and the choices and means the organisation offers for limiting its use and disclosure.

2. **Choice:** Organisations must give individuals the opportunity to choose (opt out) whether their personal information will be disclosed to a third party or used for a purpose incompatible with the purpose for which it was originally collected or subsequently authorized by the individual. For sensitive information, affirmative or explicit (opt in) choice must be given if the information is to be disclosed to a third party or used for a purpose other than its original purpose or the purpose authorized subsequently by the individual.

3. **Onward Transfer** (Transfers to Third Parties): To disclose information to a third party, organisations must apply the notice and choice principles. Where an organisation wishes to transfer information to a third party that is acting as an agent, it may do so if it makes sure that the third party subscribes to the safe harbor principles or is subject to the Directive or another adequacy finding. As an alternative, the organization can enter into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant principles.

4. **Access**: Individuals must have access to personal information about them that an organisation holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

5. **Security**: Organisations must take reasonable precautions to protect personal information form loss, misuse and unauthorised access, disclosure, alternation and destruction.

6. **Data integrity**: Personal information must be relevant for the purposes for which it is to be used. An organisation should take reasonable steps to ensure that data is

[25] See the website of U.S. Department of Commerce, Safe Harbor, available at (http://www.export.gov/safeharbor/sh_overview.html)

reliable for its intended use, accurate, complete and current.

7. **Enforcement**: In order to ensure compliance with the safe harbor principles, there must be (a) readily available and affordable independent recourse mechanisms so that each individual's complaints and disputes can be investigated and resolved and damages awarded where the applicable law or private sector initiatives so provides; (b) procedures for verifying that the commitments companies make to adhere to the safe harbor principles have been implemented; and (c) obligations to remedy problems arising out of a failure to comply with the principles. Sanctions must be sufficiently rigorous to ensure compliance by the organization. Organizations that fail to provide annual self certification letters will no longer appear in the list of participants and safe harbor benefits will no longer be assured.

Appendix III: Schedule 1 to the Personal Data (Privacy) Ordinance - Six Data Protection Principles[26]

1. Principle 1 - purpose and manner of collection of personal data

(1) Personal data shall not be collected unless —

(a) the data are collected for a lawful purpose directly related to a function or activity of the data user who is to use the data;

(b) subject to paragraph (c), the collection of the data is necessary for or directly related to that purpose; and

(c) the data are adequate but not excessive in relation to that purpose.

(2) Personal data shall be collected by means which are —

(a) lawful; and

(b) fair in the circumstances of the case.

(3) Where the person from whom personal data are or are to be collected is the data subject, all practicable steps shall be taken to ensure that —

(a) he is explicitly or implicitly informed, on or before collecting the data, of —

i. whether it is obligatory or voluntary for him to supply the data; and

ii. whether it is obligatory for him to supply the data, the consequences for him if he fails to supply the data; and

(b) he is explicitly informed —

i. on or before collecting the data, of-

(A) the purpose (in general or specific terms) for which the data are to be used; and

(B) the classes of persons to whom the data may be transferred; and

ii. on or before first use of the data for the purpose for which they were collected, of —

(A) his rights to request access to and to request the correction of the data; and

(B) the name and address of the individual to whom any such request may be made,

unless to comply with the provisions of this subsection would be likely to

[26] See Schedule 1 to the Personal Data (Privacy) Ordinance (Chapter 486 of the Laws of Hong Kong), full text of the ordinance is available at the website of the Department of Justice, Hong Kong (http://www.justice.gov.hk/Home.htm).

prejudice the purpose for which the data were collected and that purpose is specified in Part VIII of this Ordinance as a purpose in relation to which personal data are exempt from the provisions of data protection principle 6.

2. Principle 2 - accuracy and duration of retention of personal data

(1) All practicable steps shall be taken to ensure that —

(a) personal data are accurate having regard to the purpose (including any directly related purpose) for which the personal data are or are to be used;

(b) where there are reasonable grounds for believing that personal data are inaccurate having regard to the purpose (including any directly related purpose) for which the data are or are to be used —

i. the data are not used for that purpose unless and until those grounds cease to be applicable to the data, whether by the rectification of the data or otherwise; or

ii. the data are erased;

(c) where it is practicable in all the circumstances of the case to know that —

i. personal data disclosed on or after the appointed day to a third party are materially inaccurate having regard to the purpose (including any directly related purpose) for which the data are or are to be used by the third party; and

ii. that data were inaccurate at the time of such disclosure, that the third party —

(A) is informed that the data are inaccurate; and

(B) is provided with such particulars as will enable the third party to rectify the data having regard to that purpose.

(2) Personal data shall not be kept longer than is necessary for the fulfillment of the purpose (including any directly related purpose) for which the data are or are to be used.

3. Principle 3 - use of personal data

Personal data shall not, without the prescribed consent of the data subject, be used for any purpose other than —

(a) the purpose for which the data were to be used at the time of the collection of the data; or

(b) a purpose directly related to the purpose referred to in paragraph (a).

4. Principle 4 - security of personal data

All practicable steps shall be taken to ensure that personal data (including data in a form in which access to or processing of the data is not practicable) held by a data user are protected against unauthorized or accidental access, processing, erasure or other use having particular regard to —

(a) the kind of data and the harm that could result if any of those things should occur;

(b) the physical location where the data are stored;

(c) any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data are stored;

(d) any measures taken for ensuring the integrity, prudence and competence of persons having access to the data; and

(e) any measures taken for ensuring the secure transmission of the data.

5. Principle 5 - information to be generally available

All practicable steps shall be taken to ensure that a person can —

(a) ascertain a data user's policies and practices in relation to personal data;

(b) be informed of the kind of personal data held by a data user;

(c) be informed of the main purposes for which personal data held by a data user are or are to be used.

6. Principle 6 - access to personal data

A data subject shall be entitled to —

(a) ascertain whether a data user holds personal data of which he is the data subject;

(b) request access to personal data —

i. within a reasonable time;

ii. at a fee, if any, that is not excessive;

iii. in a reasonable manner; and

iv. in a form that is intelligible;

(c) be given reasons if a request referred to in paragraph (b) is refused;

(d) object to a refusal referred to in paragraph (c);
(e) request the correction of personal data;
(f) be given reasons if a request referred to in paragraph (e) is refused; and
(g) object to a refusal referred to in paragraph (f).

Appendix IV : Compliance Checks undertaken by the PCO[27]

Issues	Improvement Measures Recommended
Compliance measures taken by Hong Kong based web sites that collect personal data online	Site operators were advised to undertake immediate actions to implement compliance measures. To give practical guidance to web site operators, the PCO had prepared a guidance booklet "Preparing online Personal Information Collection Statement and Privacy Policy Statement".
Bank statements of customers transmitted by open fax to their workplace.	Unless urgency requires otherwise, the bank should deliver the documents by a more secure means such as by mail using a sealed envelop that carries the words "Personal and Confidential". To avoid inadvertent disclosure of the personal data of the customer, appropriate steps should be taken to alert the recipient of the incoming fax prior to sending the bank statements by fax.
Identification cards of persons with disability were printed with their full date of birth on the card.	There is no justifiable reason for printing the full date of birth of the cardholder on the card as verification of such information, where necessary, could be made by checking the HK Identity card. The organisations was therefore recommended to delete the full date of birth of the cardholder on future card renewal or printing.
Papers containing personal data of individuals were re-used for photocopying and distributed to unrelated parties	The department was recommended to implement guidelines to remind all staff to avoid re-using papers that contain personal data of individuals unless appropriate measures are taken to safeguard those data from inadvertent disclosure.
A prize-winning announcement made on an Internet web-site disclosed the full name and HK Identity card number of prize-winners.	The oganisation was recommended to publish either the name of winners or the HK Identity card number in its future prize-winning announcements. Where both data are published, it should avoid disclosing the full HK Identity card number of prize-winner.

[27] Information on other compliance checks are available at the 2001-02 Annual Report published by the PCO, available at its website (http://www.pco.org.hk/english/publications/annualreport.html).

Issues	Improvement Measures Recommended
Job applicants were required to provide a copy of their HK Identity card when they attended a job interview.	Copies of the HK Identity card should only be collected from prospective employees after they have accepted employment. As proof of compliance on the part of the employer with section 17J of the Immigration Ordinance. The company was recommended to cease the practice.
Visitors to a building estate car park were required to provide their HK Identity card number for recording when leaving the car park.	The car park management was recommended to consider adopting a "double permit system" in which an exit pass given to the driver on entry to the car park must be surrendered upon departure from the car park.
Notices issued to registered consumers responsible for repair of building communal pipeworks listed the names and mailing addresses of other parties	The department was recommended to revise the repair notice so as to avoid the listing of the names and mailing addresses of other responsible parties. When the mailing address of a registered consumer differs from the address of the concerned premises, a personal copy of the notice should be sent instead.

Appendix V : Matching Procedures Applications Approved by the PCO[28]

Requesting Party	Related matching procedures that were approved
Treasury Department	To identify government pensioners in receipt of both salaries and pension payments by comparing personal data of pensioners who received pension payments with personal data of civil servants who were in receipt of salaries and allowances.
Social Welfare Department	To detect overpayment of social security payments to social benefits applicants/recipients who might be ineligible to receive them by comparing their personal data with personal data held by the Treasury Department in respect of civil servants who are in receipt of salary/pension; the Correctional Services Department in respect of inmates of prison facilities; the Land Registry in respect of property owners who have ownership of properties; and the Companies Registry in respect of company directors who have asset or income derived from holding a company.
Hospital Authority Treasury Department Chinese University of Hong Kong The Hong Kong University of Science & Technology	To prevent double housing benefits being obtained contrary to double housing benefits rule by comparing personal data of housing benefits applicants/recipients and their spouse held by individual public sector organization with personal data of public housing benefits recipients maintained by the Housing Authority
Inland Revenue Department	To identify instances of taxpayers omitting or understating their source of funds obtained to finance the purpose of properties by comparing the taxpayers' personal data collected in their tax returns with data collected for the purpose of stamp duty assessment.

[28] Information on other matching procedures are available at the 2001-02 Annual Report published by the PCO, available at its website (http://www.pco.org.hk/english/publications/annualreport.html).

Requesting Party	**Related matching procedures that were approved**
Registration and Electoral Office	To identify registered electors who might become ineligible to vote, to stand for election or to register as an elector as a result of their change in permanent residency status by comparing their personal data with personal data maintained by the Registration of Persons database of the Immigration Department To enforce the eligibility status of registered voters who have claimed to have changed their residential address by comparing their personal data with personal data of public housing tenants or owners maintained by the Housing Authority
Mandatory Provident Fund Authority	To enforce enrolment requirements of the Mandatory Provident Fund Schemes Ordinance in respect of self-employed persons by comparing their personal data enrolled in registered schemes of Trustees with personal data of subjects who have registered self-employed business with the Business Registration Office of the Inland Revenue Department
Food and Environmental Hygiene Department	To enforce the requirements of section 38 of the Hawker Regulations and to identify potential cases of conflict of interest of serving staff who might be holders of a fixed-pitch hawker licence by comparing personal data of staff personnel records with data held in the hawker licence records system.